UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
09/328,726	10/26/98	COLLINS T	10577-404-1U

LM02/0427

ROBERT J BENNETT
TOWNSEND AND TOWNSEND AND CREW LLP
8TH FLOOR
TWO EMBARCADERO CENTER
SAN FRANCISCO CA 94111-3834

EXAMINER	
LEANING, J	
ART UNIT	**PAPER NUMBER**
2766	6

DATE MAILED: 04/27/00

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary	**Application No.** 09/328,726	**Applicant(s)** COLLINS ET AL.
	Examiner Jeffrey S Leaning	**Art Unit** 2766

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).

Status

1)☒ Responsive to communication(s) filed on *26 October 1998* .

2a)☐ This action is **FINAL.** 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *14-16* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *14-16* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claims _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

a)☐ All b)☐ Some * c)☐ None of the CERTIFIED copies of the priority documents have been:

1.☐ received.

2.☐ received in Application No. (Series Code / Serial Number) _____ .

3.☐ received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. & 119(e).

Attachment(s)

14) ☒ Notice of References Cited (PTO-892)

15) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)

16) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .

17) ☐ Interview Summary (PTO-413) Paper No(s). _____ .

18) ☐ Notice of Informal Patent Application (PTO-152)

19) ☐ Other: .

DETAILED ACTION

Claims 1-13 have been canceled by the applicants. Claims 14-16 are rejected herein.

Due to the notation-intensive nature of the application, the examiner will state the conventions that he will use. Underscore marks will denote subscripts, so 'a sub b' will be denoted by 'a_b'. Carets will denote superscripts, so 'a to the b' will be denoted by 'a^b'.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claim 16 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a. Claim 16 includes a term M_(I'). This term is left undefined and is unknown to one of ordinary skill in the art. It would require undue experimentation to determine M_(I') and make or use the invention. For the purposes of this examination, the examiner interprets M_(I') to mean M_i.

b. In line 23 of claim 16 the applicant cites C_1. This term is left undefined and is unknown to one of ordinary skill in the art. It would require undue experimentation to determine

C_1 and make or use the invention. For the purposes of this examination, the examiner interprets C_1 to mean C.

Double Patenting

3. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970);and, *In re Thorington,* 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321© may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

4. Claims 14-16 rejected under the judicially created doctrine of double patenting over claims 1-13 of U. S. Patent No. 5,848,159 since the claims, if allowed, would improperly extend the "right to exclude" already granted in the patent.

The subject matter claimed in the instant application is fully disclosed in the patent and is covered by the patent since the patent and the application are claiming common subject matter, as follows: Claim 8 of U. S. Patent No. 5,848,159 refers to a “succession of invertible operations” which the specification reveals in column 6 lines 1-67 to column 7 lines 1-33 to be the very same operations given by the equations in the claims of the present application.

Furthermore, there is no apparent reason why applicant was prevented from presenting claims corresponding to those of the instant application during prosecution of the application which matured into a patent. See *In re Schneller*, 397 F.2d 350, 158 USPQ 210 (CCPA 1968). See also MPEP § 804.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 14-16 rejected under 35 U.S.C. 103(a) as being unpatentable over Kawamura *et al* (US 5,046,094) in view of Menezes *et al.*

a. Claim 14 is directed to a method for establishing cryptographic communications. Kawamura teaches of a computation method for processing secret information, see the abstract.

i. Both Kawamura *et al* and the applicants use RSA-type cryptography. This cryptography employs a modulus consisting of a product of prime numbers. In the case of Kawamura *et al*, there are two numbers in the modulus and they are called 'p' and 'q'. In the cases of the applicants and Menezes *et al*, there are possibly more than two prime numbers in the modulus and they are called p_1, p_2, ... , p_n. Hence, p corresponds to p_1, and q corresponds to p_2. This is merely notation, and the examiner point it out for the sake of clarity.

ii. Kawamura *et al* teach of encoding a plaintext word M to a ciphertext word C where M is less than or equal to n-1 where n is the product of two primes, see column 1 line 46.

iii. Kawamura *et al* teach of transforming ciphertext C to message M, see the abstract.

iv. Kawamura *et al* teach of calculating the quantities of lines 14-25 of claim 14, see equations (18), (19), (24) and (25) in columns 8-10 of Kawamura *et al*. The following correspondences hold, setting I=2 for the sake of clarity. The applicants' p_1 corresponds to Kawamura *et al*'s p. The applicants' p_2 corresponds to Kawamura *et al*'s q. The applicants' e_1 corresponds to Kawamura *et al*'s r_p. The applicants' e_2 corresponds to Kawamura *et al*'s r_q. The applicants' C_1 corresponds to Kawamura *et al*'s X_p. The other correspondences are analogous.

v. The number 'e' is selected as being relatively prime to the described lcm (least common multiple), see column 1 lines 24-50.

vi. Kawamura *et al* calculate the last two quantities of claim 14 (lines 28 and 29), see the numbered equations of Kawamura *et al*: (21)-(26) in columns 9-10. The following correspondences hold, setting I=2 for the sake of clarity. The applicants' p_1 corresponds to Kawamura *et al*'s p. The applicants' p_2 corresponds to Kawamura *et al*'s q. The applicants' w_2 corresponds to Kawamura *et al*'s p. The applicants' (w_2^-1 mod p_2)mod p_1]p_1 mod n corresponds to Kawamura *et al*'s w_q=p(p^-1 mod q) mod n. And of course, the applicants' M corresponds to Kawamura *et al*'s M and the applicants' C corresponds to Kawamura *et al*'s C.

vii. Kawamura *et al* lack a teaching that there can be more than two primes in the modulus and that the message M is transformed to ciphertext C using the steps described in paragraphs 6.a.iii-vi above.

(1) The examiner takes official notice that encryption and decryption are inverse operations. It would be obvious to one of ordinary skill in the art to use the above steps for encryption because inverse operations are performed using the steps in an inverse manner.

(2) Menezes *et al* teach that the RSA encryption problem relies on the difficulty of the integer factorization problem, see the introduction to section 3.2. Menezes *et al* further teach that the integer factorization problem comes from factoring the product of multiple primes p_1^e1 p_2^e2 ... p_k^ek, see definition 3.3. It would be obvious for one of ordinary skill in the art to modify the system of Kawamura *et al* to have a modulus having the number of primes, 'k', being a number greater than 2.

b. Claim 15 differs from claim 14 in that the message is decrypted using the corresponding formulae and steps. See the above.

c. Claim 16 is directed to a cryptographic communications system. Kawamura *et al* teach of a distributed secret information processing unit, corresponding to the applicants' cryptographic communications system, see the abstract.

i. Both Kawamura *et al* and the applicants use RSA-type cryptography. This cryptography employs a modulus consisting of a product of prime numbers. In the case of Kawamura *et al*, there are two numbers in the modulus and they are called 'p' and 'q'. In the cases of the applicants and Menezes *et al*, there are possibly more than two prime numbers in the modulus and they are called p_1, p_2, ... , p_n. Hence, p corresponds to p_1, and q corresponds to p_2. This is merely notation, and the examiner point it out for the sake of clarity.

ii. Kawamura *et al* teach of an encrypting means and a communication medium, see the abstract.

iii. Kawamura *et al* teach of enciphering a message in the manner of the applicants, using the formula of line 13 of the claim, see column 1 line 46.

iv. The number 'e' is selected as being relatively prime to the described lcm (least common multiple), see column 1 lines 24-34.

v. Kawamura *et al* teach of a decoding means for receiving C and transforming C, see the abstract.

vi. Kawamura *et al* calculate the last two quantities of claim 16 (lines 21-23), see the numbered equations of Kawamura *et al*: (21)-(26) in columns 9-10. The following correspondences hold, setting I=2 for the sake of clarity. The applicants' p_1 corresponds to

Kawamura *et al*'s p. The applicants' p_2 corresponds to Kawamura *et al*'s q. The applicants' w_2 corresponds to Kawamura *et al*'s p. The applicants' Y_1 corresponds to Kawamura *et al*'s C. The applicants' (w_2^-1 mod p_2)mod p_1]p_1 mod n corresponds to Kawamura *et al*'s w_q=p(p^-1 mod q) mod n. And of course, the applicants' M corresponds to Kawamura *et al*'s M and the applicants' C corresponds to Kawamura *et al*'s C.

vii. Kawamura *et al* lack a teaching that there can be more than two primes in the modulus. Menezes *et al* teach that the RSA encryption problem relies on the difficulty of the integer factorization problem, see the introduction to section 3.2. Menezes *et al* further teach that the integer factorization problem comes from factoring the product of multiple primes p_1^e1 p_2^e2 ... p_k^ek, see definition 3.3. It would be obvious for one of ordinary skill in the art to modify the system of Kawamura *et al* to have a modulus having the number of primes, 'k', being a number greater than 2.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Quisquater *et al* teaches of using the Chinese Remainder Theorem (as the applicants do to derive the formulas in the claims) in association with RSA cryptography and cites many benefits, see formula (1) on pp. 906 in particular. Naciri (US 5,761,310) also teaches of using formulas corresponding to the applicants' in the same setting, see figure 3 for example.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jeffrey S. Leaning whose telephone number is (703) 306-5975. The examiner can normally be reached on weekdays from 9:00am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes, can be reached on (703) 305-9711. The fax phone number for the organization where this application or proceeding is assigned is (703) 308-9051.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Jeffrey S. Leaning
19 April 2000

GAIL O. HAYES
SUPERVISORY PATENT EXAMINER
GROUP 2700